PN513'58

(12) UK Patent Application (19) GB (11) 2 387 681 (13) A

(43) Date of A Publication 22.10.2003

(21) Application No 0208916.7

(22) Date of Filing 18.04.2002

(71) Applicant(s)
Isis Innovation Limited
(Incorporated in the United Kingdom)
Ewert House, Ewert Place, Summertown,
OXFORD, OX2 7SG, United Kingdom

(72) Inventor(s)
John Heasman
Steve Moyle

(74) Agent and/or Address for Service
Urquhart-Dykes & Lord
Alexandra House, 1 Alexandra Road,
SWANSEA, SA1 5ED, United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition V)
G4A AFGN AFMG

(56) Documents Cited
WO 2002/027443 A **WO 2001/099372 A**
WO 2001/031420 A **US 6370648 A**

(58) Field of Search
UK CL (Edition T) **G4A** AFGN AFMG
INT CL[7] **G06F** 1/00
Other: **Online; EPODOC, JAPIO, WPI.**

(54) Abstract Title
Intrusion detection system with inductive logic means for suggesting new general rules

(57) An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring the activity relative to the computer system or network, means for receiving and storing one or more general rules, each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion, and matching means for receiving data relating to activity relative to said computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the one or more general rules to identify an intrusion or attempted intrusion. Inductive logic techniques are proposed for suggesting new intrusion detection rules for inclusion into the system, based on examples of sinister traffic.

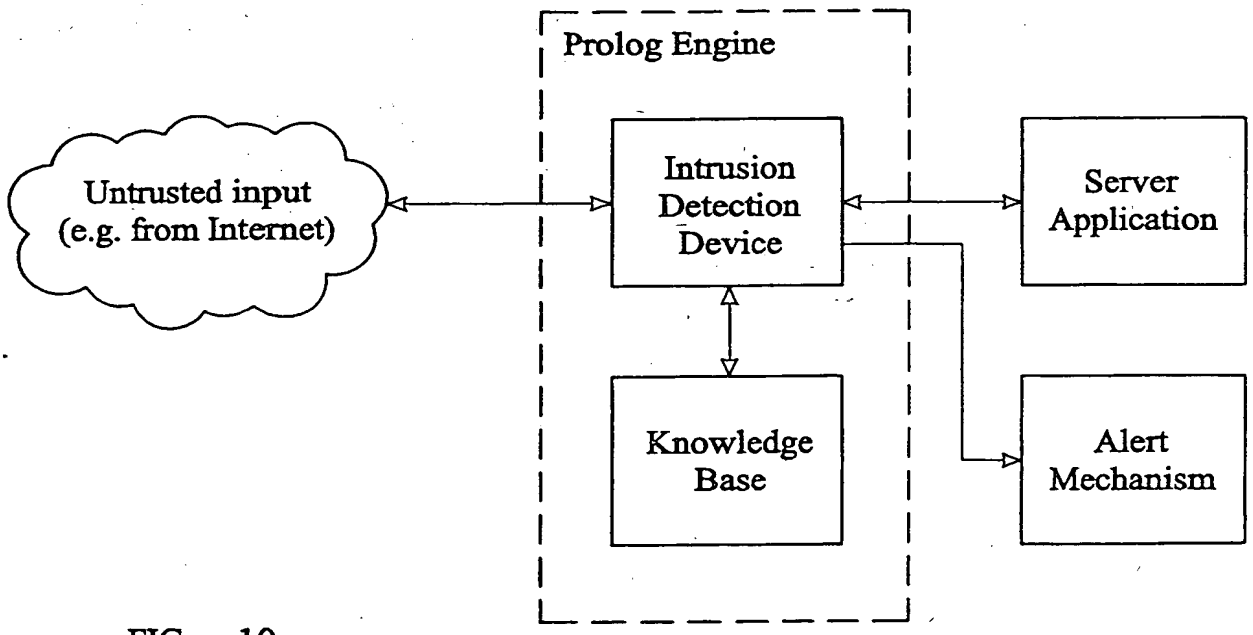

FIG. 10

GB 2 387 681 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Application No: GB 0208916.7
Claims searched: 1 - 8

Examiner: David P Maskery
Date of search: 12 November 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A (AFGN, AFMG)

Int Cl (Ed.7): G06F (1/00)

Other: Online; EPODOC, JAPIO, WPI.

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	WO 02/27443 A2	(ITT MANUFACTURING) See page 15 lines 10 - 28, page 16 lines 11 - 20 and page 18 lines 6 - 28	1, 2, 6 and 7
X	WO 01/99372 A2	(SECURIFY, INC) See pages 17, 18, 26, 27, 30, 32, 33, 34, 38, 56, 100 and 159 - 162	1 - 7
X	WO 01/31420 A2	(VISA INTERNATIONAL SERVICE ASS) See pages 6 - 8 and 11	1, 2, 6 and 7
X	US 6370648 B1	(VISA INTERNATIONAL SERVICE ASS) See columns 3 and 4.	1, 2, 6 and 7

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.